

Grandstream Networks, Inc.

GWN76xx Wi-Fi Access Points

Master/Slave Architecture Guide



Table of Contents

INTRODUCTION.....	4
DISCOVER AND PAIR GWN76XX ACCESS POINTS	5
Discover GWN76xx	5
<i>Method 1: Discover GWN76xx using its MAC address.....</i>	<i>5</i>
<i>Method 2: Discover GWN76xx using GWN Discovery Tool.....</i>	<i>6</i>
Pair Slave GWN76xx Access Points	7
Configure Failover Master.....	9
<i>Failover Master Overview.....</i>	<i>9</i>
<i>Set a Failover Master</i>	<i>10</i>
<i>Failover Mode.....</i>	<i>11</i>
CREATE AND MANAGE NETWORK GROUPS	14
Network Group & SSID Configuration	15
Additional SSID	20



Table of Figures

Figure 1: GWN76XXs Setup sample	4
Figure 2: Discover the GWN76xx using its MAC Address	5
Figure 3: GWN Discovery Tool	6
Figure 4: Discover AP	7
Figure 5: Discovered Devices	7
Figure 6: GWN76xx online	8
Figure 7 : Failover Architecture	10
Figure 8 : Configure Failover	10
Figure 9 : Select MAC for Failover	11
Figure 10 : Provisioning Failover Master	11
Figure 11 : Failover Mode Web Login	12
Figure 12 : Failover Overview	12
Figure 13 : Switch to Master	13
Figure 14 : AP Switched to Master	13
Figure 15: Network Group	14
Figure 16: Add a New Network Group	14
Figure 17: Wi-Fi Settings	18
Figure 18: Device Membership	19
Figure 19: Add AP to Network Group from Access Points Page	19
Figure 20: WiFi Schedule Feature	20
Figure 21: Additional SSID	21
Figure 22: Additional SSID Created	21

Table of Tables

Table 1: Device Configuration	8
Table 2: Network Group Settings – Basic	15
Table 3: Network Group Settings – Wi-Fi	16



INTRODUCTION

The GWN76xx Wireless Access Points Series can be deployed in a network environment as standalone (using only one GWN76xx to provide wireless network access) or in Master/Slave architecture (using multiple GWN76xx units) to extend wireless network access range.

In Master/Slave configuration, a unique/chosen GWN76xx acts as master/controller and can manage (up to 50 when using GWN7610 as Master and up to 30 when using GWN7600 as Master) other GWN76xx series considered as slaves. Note that master GWN7600 can act as controller and can also be member of network group(s).

This guide covers Master/Slave architecture mode giving steps to successfully configure GWN76xx access points in your network environment; including steps to discover and pair GWN76xx units, create and manage network groups and SSIDs.

The figure below shows a sample setup of a GWN7610 master with different slave units, and connected Wi-Fi clients through different SSIDs defined in network groups.

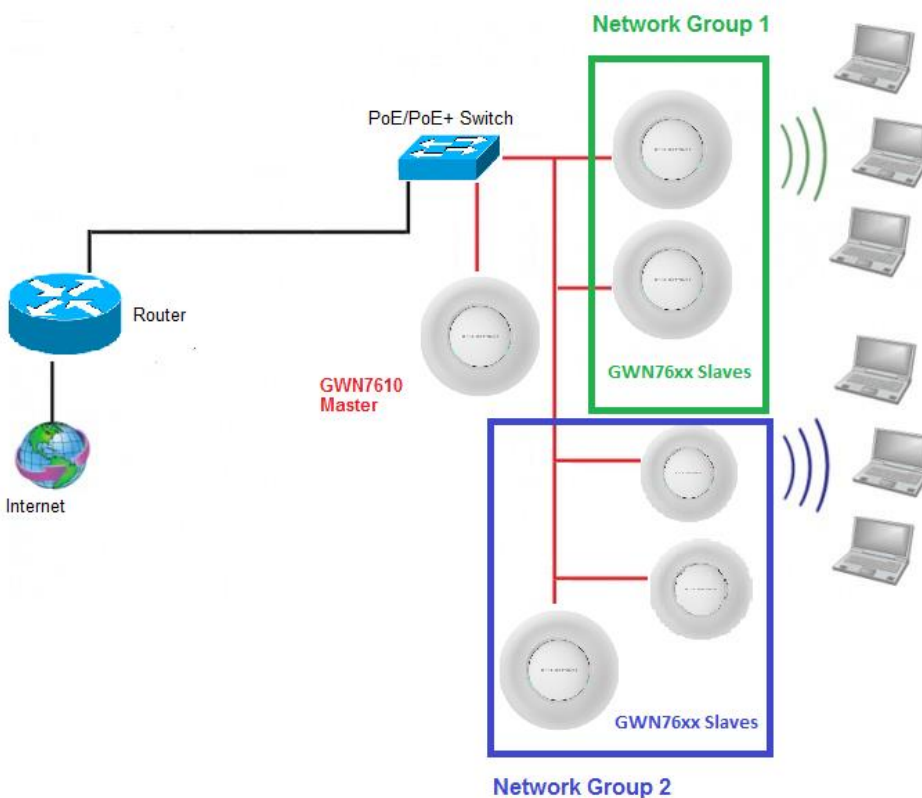


Figure 1: GWN76XXs Setup sample



DISCOVER AND PAIR GWN76XX ACCESS POINTS

In this guide, we will consider an environment where different GWN76xx access points models are installed, one of them will be Master over the remaining ones (Slaves) as shown in Figure 1.

To set a GWN76xx as Master, we need to access to its web interface by discovering it first on the network.

The following chapter describes two methods how to discover a GWN76xx connected to network and configure it as Master.

Discover GWN76xx

Once the GWN76xx is powered up and connected to the network correctly, it can be discovered using one of the following methods:

Method 1: Discover GWN76xx using its MAC address

1. Locate the MAC address on the MAC tag of the unit, which is on the underside of the device, or on the package.
2. From a computer connected to same network as the GWN76xx, type in the following address [https://gwn_\[MAC_address\].local/](https://gwn_[MAC_address].local/) using the GWN76xx's MAC address on your browser.

For example, if a GWN7610 has the MAC address **00:0B:82:8B:4E:28**, this unit can be accessed by typing https://gwn_000b828b4e28.local/ on the browser.

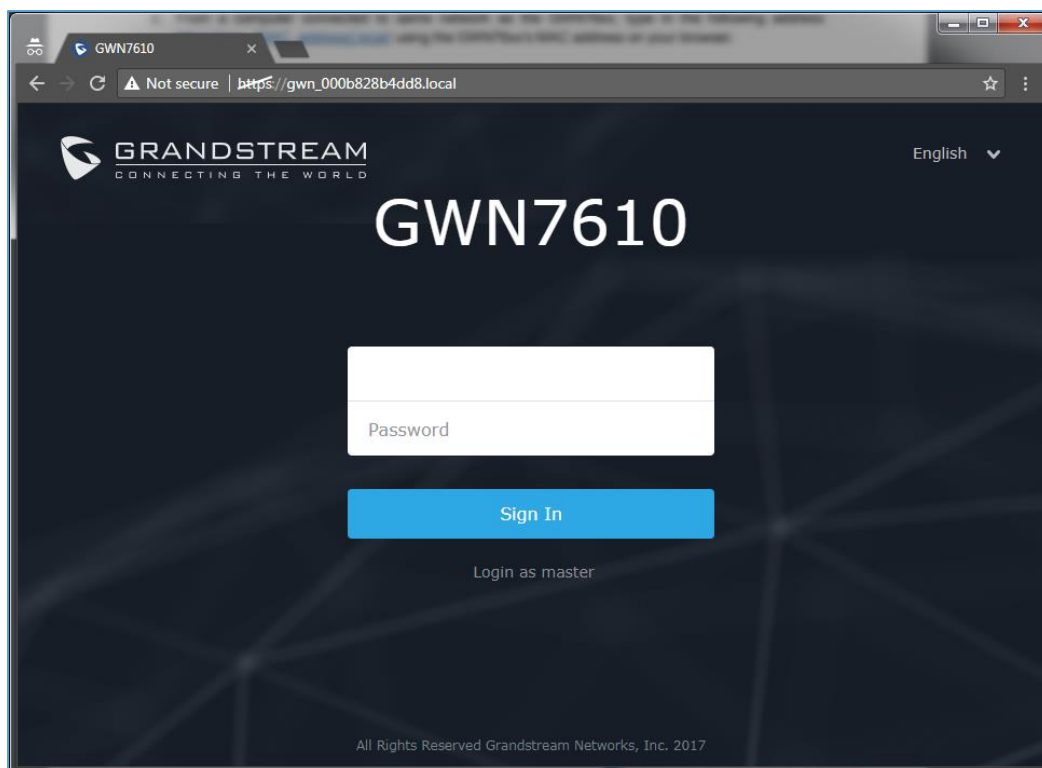


Figure 2: Discover the GWN76xx using its MAC Address



Method 2: Discover GWN76xx using GWN Discovery Tool

1. Download and install **GWN Discovery Tool** from the following link:
<http://www.grandstream.com/sites/default/files/Resources/GWNDiscoveryTool.zip>
2. Open the “GWN Discovery Tool”, click on **Select** to define the network interface, then click on **Scan**.
3. The tool will discover all GWN76xx Access Points models connected on the network showing their MAC, IP addresses and firmware version.
4. Click on **Manage Device** to be redirected directly to the GWN76xx's configuration interface, or type in manually the displayed IP address on your browser.

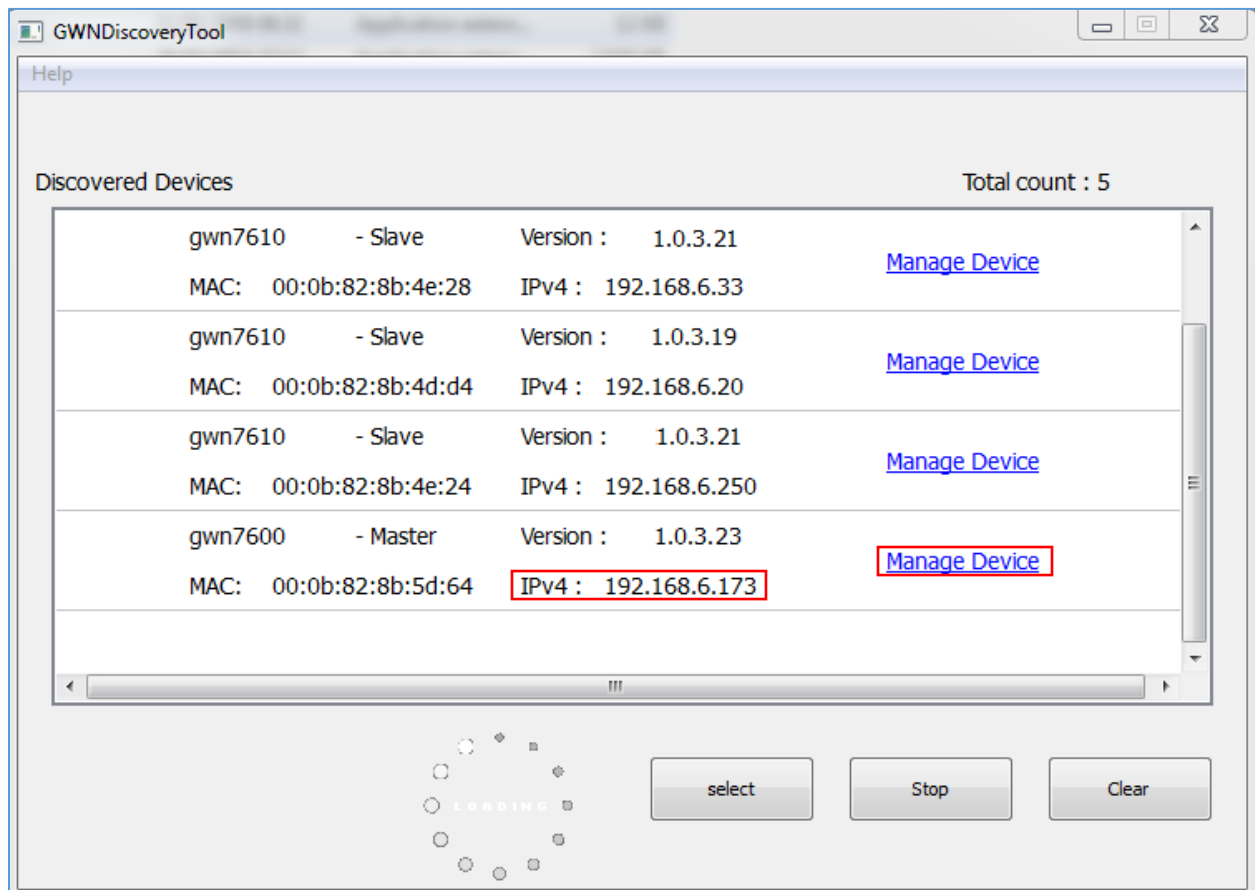


Figure 3: GWN Discovery Tool

Notes:

- At first boot or after factory reset, users will be asked to change the default administrator and user passwords before accessing GWN76xx web interface. The new password fields are case sensitive with a maximum length of 32 characters. Using strong passwords including letters, digits and special characters are recommended for better security.
- At factory reset, “**Set unit as Master**” will be checked by default, click on “**Sign In**” after typing the admin’s username and password as shown above.



Pair Slave GWN76xx Access Points

To pair a GWN76xx access points (slaves) connected to the same network as the Master GWN76xx follow the below steps:

1. Connect to the GWN76xx Web GUI as Master and go to **Access Points**.

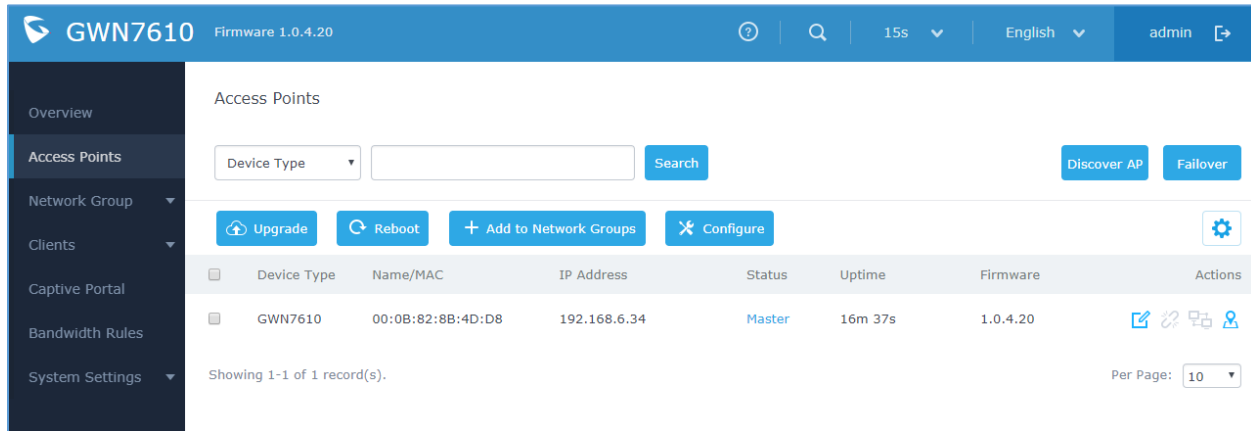




Figure 4: Discover AP

2. Click on **Discover AP** button in order to discover different GWN76xx access points models within GWN76xx's Network, the following page will appear.

Device Type	MAC	IP Address	Firmware	Actions
GWN7610	00:0B:82:8B:4E:28	192.168.6.33	1.0.3.21	[Link]
GWN7610	00:0B:82:8B:4D:D4	192.168.6.20	1.0.3.15	[Link]
GWN7610	00:03:7F:11:11:11	192.168.6.251	1.0.3.19	[Link]

Figure 5: Discovered Devices

3. Click on **Pair**  under Actions, to pair the discovered Access Point as Slave with the GWN76xx acting as Master.
4. The paired GWN76xx will appear Online, click on  to unpair it.



Access Points

Device Type Search Discover AP Failover

Upgrade Reboot + Add to Network Groups ✕ Configure ⚙️

<input type="checkbox"/>	Device Type	Name/MAC	IP Address	Status	Uptime	Firmware	Actions
<input type="checkbox"/>	GWN7610	00:0B:82:8B:4E:24	192.168.6.251	Master	17m 59s	1.0.3.21	
<input type="checkbox"/>	GWN7610	00:0B:82:8B:4D:D8	192.168.6.26	Online	7m 59s	1.0.3.19	

Showing 1-2 of 2 record(s). Per Page: 10

Figure 6: GWN76xx online


5. Click on  next to Master or paired access point to check device configuration for its status, clients connected to it and configuration. Refer to below table for Device Configuration tabs.

Table 1: Device Configuration

Status	Shows the device's status information such as firmware version, IP address, link speed, uptime and users count via different Radio channels.
Clients	Shows the connected users to the GWN76xx access point.
Configuration	<ul style="list-style-type: none"> • Device Name: Set GWN76xx's name to identify it along with its MAC address. • Fixed IP: Used to set a static IP for the GWN76xx, if checked, the following fields will need to be configured: <ul style="list-style-type: none"> ▪ IPv4 Address: Enter the IPv4 address to be set as static for the device. ▪ IPv4 Subnet Mask: Enter the Subnet Mask. ▪ IPv4 Gateway: Enter the Network Gateway's IPv4 Address. ▪ Preferred IPv4 DNS: Enter the Primary IPv4 DNS. ▪ Alternate IPv4 DNS: Enter the Alternate IPv4 DNS. • Frequency: Set the GWN76xx's frequency, it can be either 2.4GHz, 5GHz or Dual-band. • Enable Band Steering: When Frequency is set to Dual-Band, checking this option will enable Band Steering on the Access Point, this will help redirecting clients to 5GHz radio band if supported on the device (otherwise, 2.4GHz radio band will be used) for efficient use and to benefit from the maximum throughput. • Mode: Choose the mode for the frequency band, 802.11n/g/b for 2.4Ghz and 802.11ac for 5Ghz. • Channel Width: Choose the Channel Width. Note that Wide channel will give better speed/throughput, and narrow channel will have less interference. 20Mhz is suggested in very high density environment. • 40MHz Channel Location: Configure the 40MHz channel location when using 20MHz/40MHz in Channel Width; it can be set to "Secondary Below Primary", "Primary Below Secondary" or "Auto".



- **Channel:** Select “Auto” or a specific channel. Default is “Auto”. Note that the proposed channels depend on **Country** Settings under **System Settings**→**Maintenance**→**Basic**.
- **Enable Short Guard Interval:** Check to activate this option to half the guard interval (from 800ns to 400ns) ensuring that distinct transmissions do not interfere with one another, this will help increasing throughput.
- **Active Spatial Streams:** Choose active spatial stream. Available options: “Auto”, “1 stream”, “2 streams” and “3 streams” (3 streams are supported on GWN7610 model only).
- **Radio Power:** Set the Radio Power depending on desired cell size to be broadcasted, three options are available: “Low”, “Medium” or “High”. Default is “High”.
- **Allow Legacy Devices (802.11):** check this option to allow legacy WiFi devices to connect to the AP using 802.11b norm.
- **Custom Wireless Power:** Enter custom value of power (expressed in dBm).

Note: If a GWN76xx is not being paired or pair icon is grayed, make sure that it is not already paired with another GWN76xx Master Access Point. If yes, it needs to be unpaired first, or reset to factory default settings in order to make it available for pairing by other GWN76xx Access Point Controller.

Configure Failover Master

Failover Master Overview

For redundancy and backup function, the GWN76XX access points are now supporting Failover Master function, users can specify a slave AP as failover master. Whenever it detects the master is down, it will promote itself to be as failover master.

In order to avoid a single point of failure in a wireless network, and for redundancy and failover function, users are able to configure a slave AP as failover master, this slave AP will be the replacing the Master in its functions, and will promote itself as failover master within a time frame of around 20~30 minutes by entering failover mode, after then, if the master AP comes back, failover master will automatically go back to slave mode.

The Failover architecture is as follow:



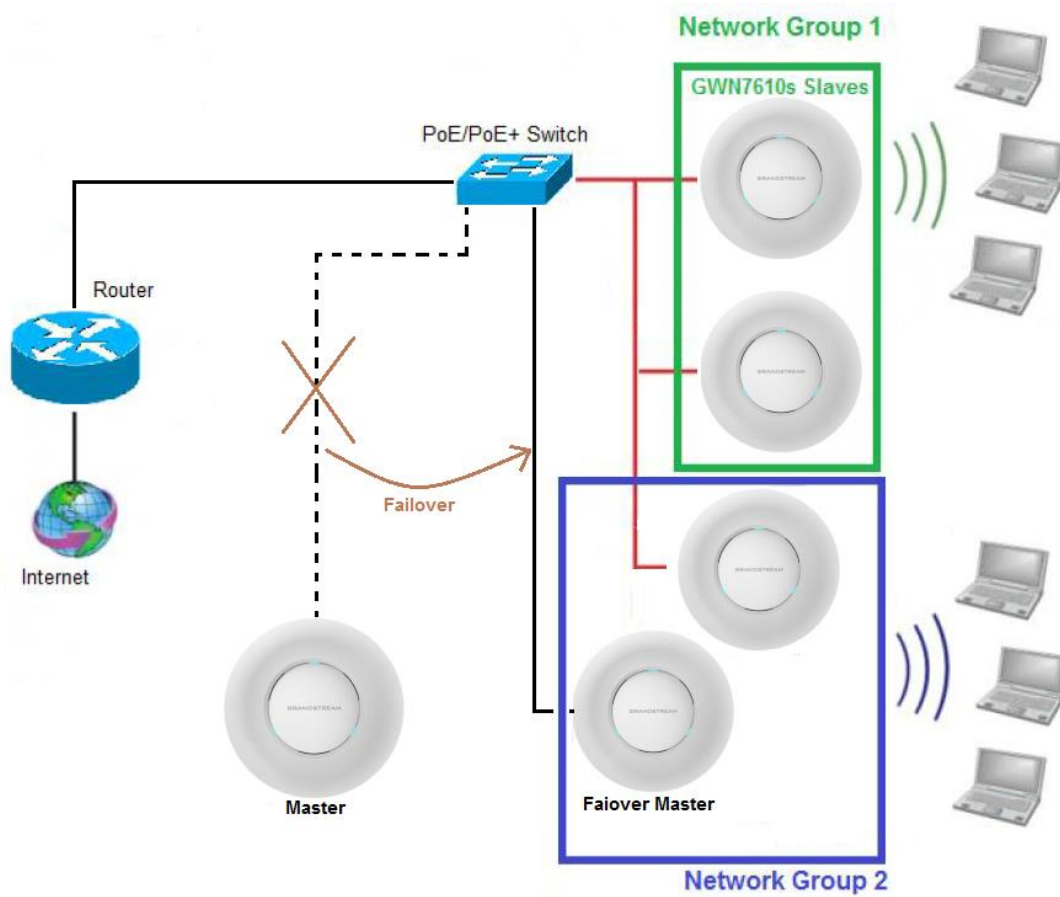


Figure 7 : Failover Architecture

Set a Failover Master

Users can select the failover Master by following below steps:

1. Log into web GUI of the master GWN, and go to **Access Points**, then click on **Failover** as follow:

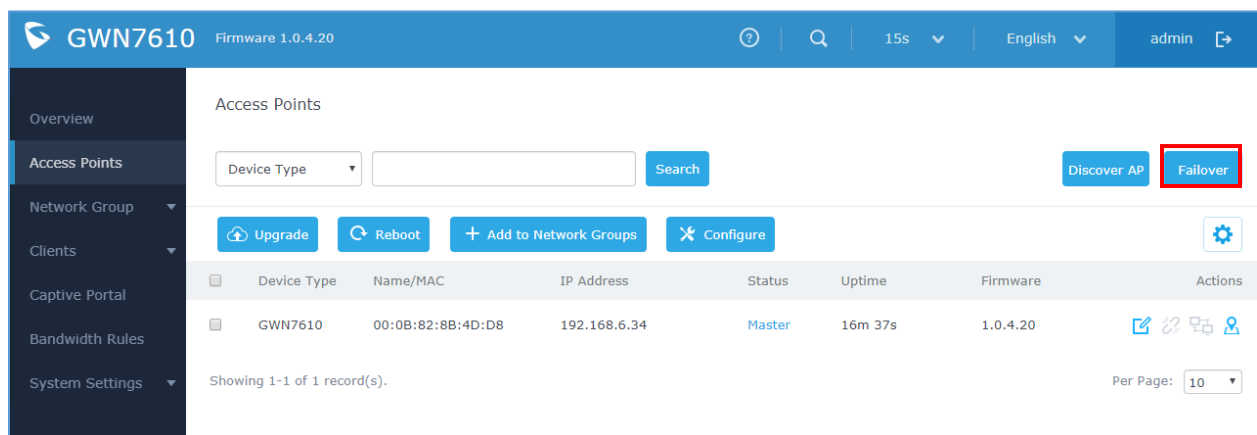


Figure 8 : Configure Failover

- Once Failover is pressed, following window will pop up, set one AP as Failover by selecting its MAC Address:

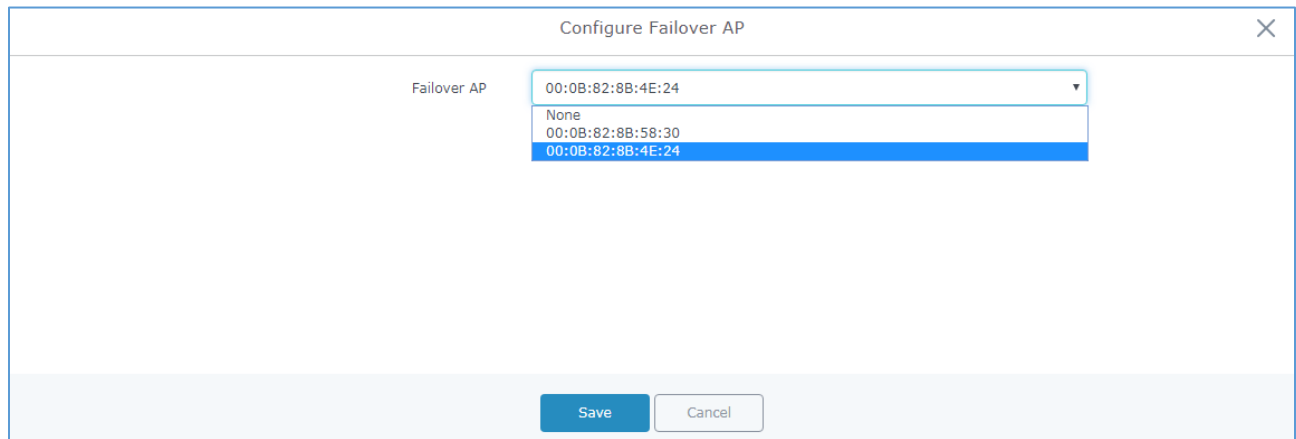
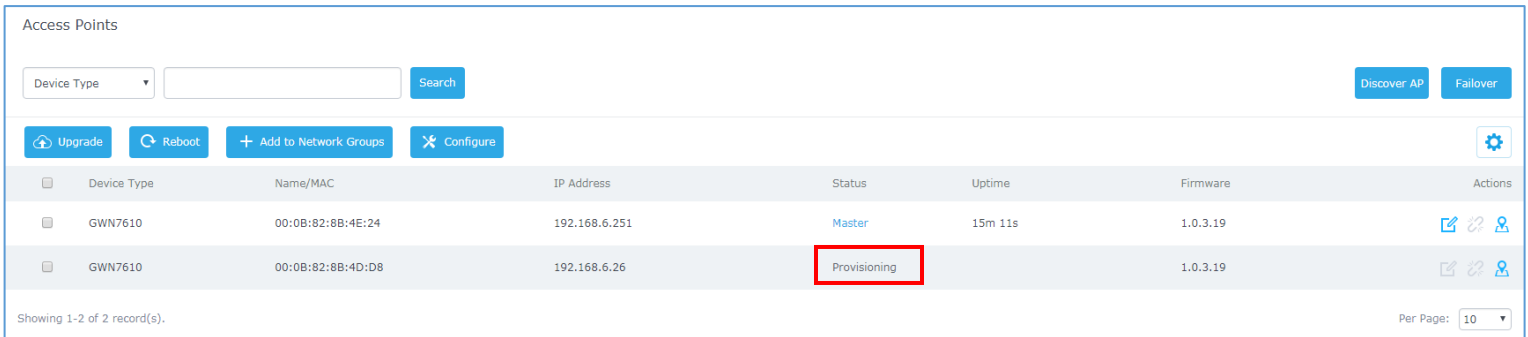


Figure 9 : Select MAC for Failover

- Press **Save** then **Apply Changes**.

Once the Failover master is selected, the Master will provision the selected AP with the needed network configuration as illustrated in the following screenshot:









Device Type	Name/MAC	IP Address	Status	Uptime	Firmware	Actions
GWN7610	00:0B:82:8B:4E:24	192.168.6.251	Master	15m 11s	1.0.3.19	  
GWN7610	00:0B:82:8B:4D:D8	192.168.6.26	Provisioning		1.0.3.19	  

Figure 10 : Provisioning Failover Master

When done, the selected AP status will change to **ONLINE**, this AP will keep monitoring the Master and will be promoted as Failover when the primary Master is no more responding.

Failover Mode

As explained previously, once failover slave has been selected, the primary master will send the configuration of the network to the failover slave, and the slave will start monitoring the status of the primary master to detect any failure for any reason (network connection loss, power outage).

In case of failure, the failover slave will promote itself to a temporary backup master while waiting for the primary master to recover.

During the failover mode, users could access the web GUI of the failover slave using a special failover account with same admin password.

- Username = **failover**
- Password = **admin password**



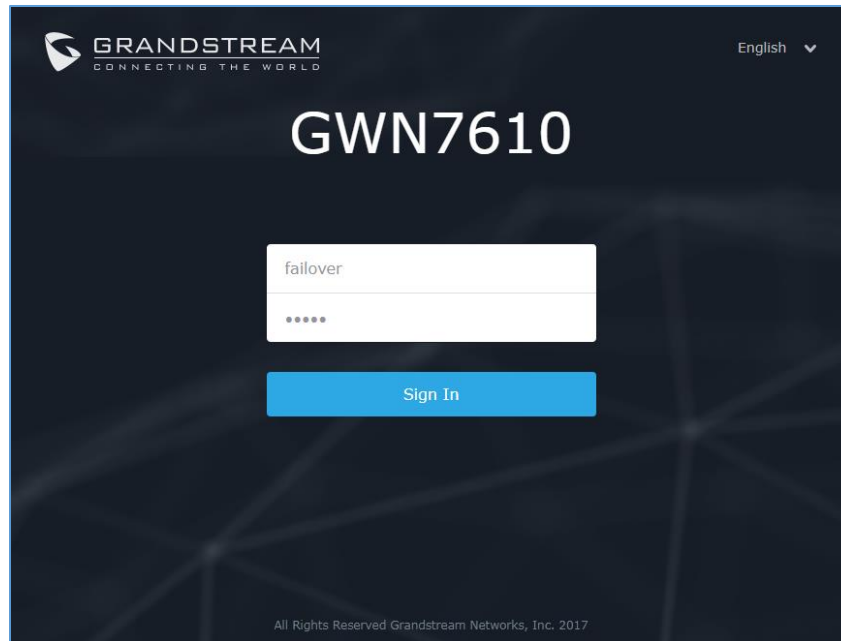


Figure 11 : Failover Mode Web Login

Once done, users will have access to the AP in Failover mode as displayed in the following screenshot:

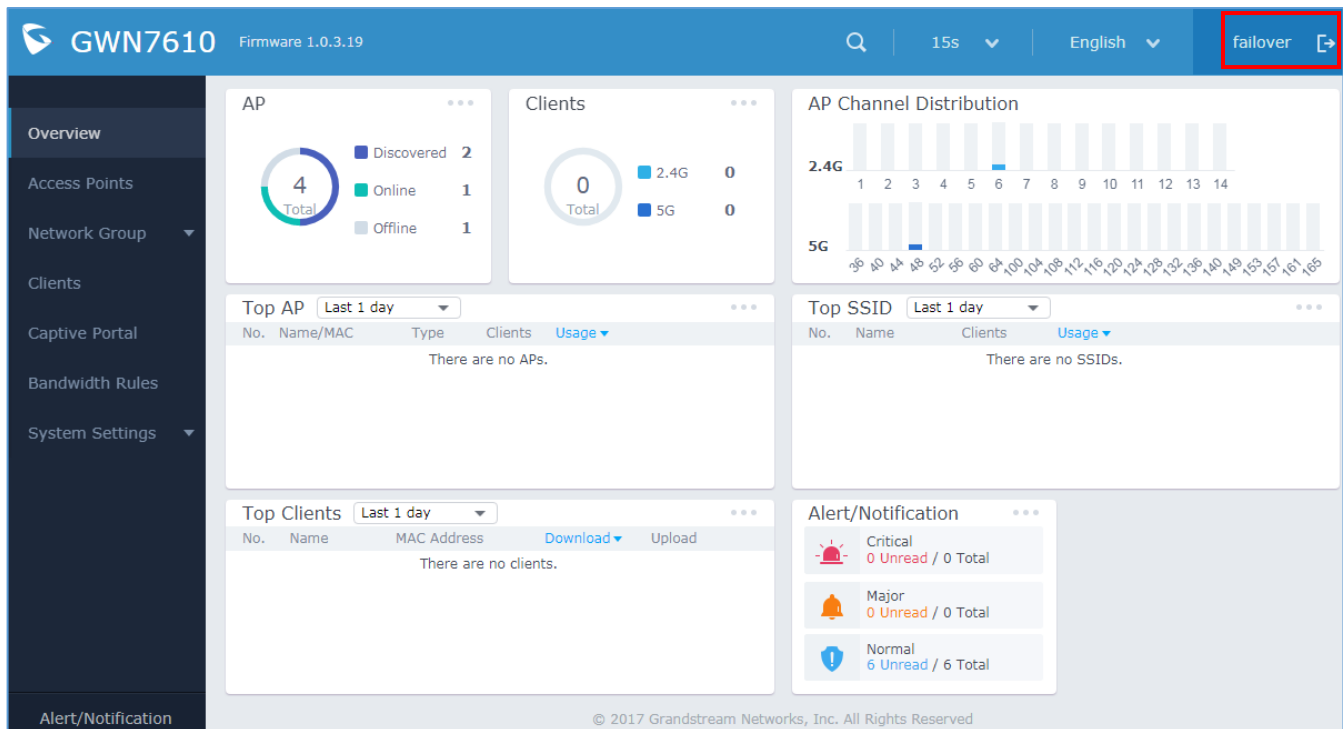


Figure 12 : Failover Overview

The failover mode has only read permission on the configuration and very limited options, users still can reboot other slave Access points in case it is needed.

At this stage, the AP will keep monitoring the primary Master, and will automatically go back to slave mode when it detects the recovery of the primary Master.



The AP is now in Failover mode, and it's acting as the primary Master, this can be illustrated in the AP status when accessing Access Points board, a new option “**Switch to master**” will be added to the board in the top right corner:

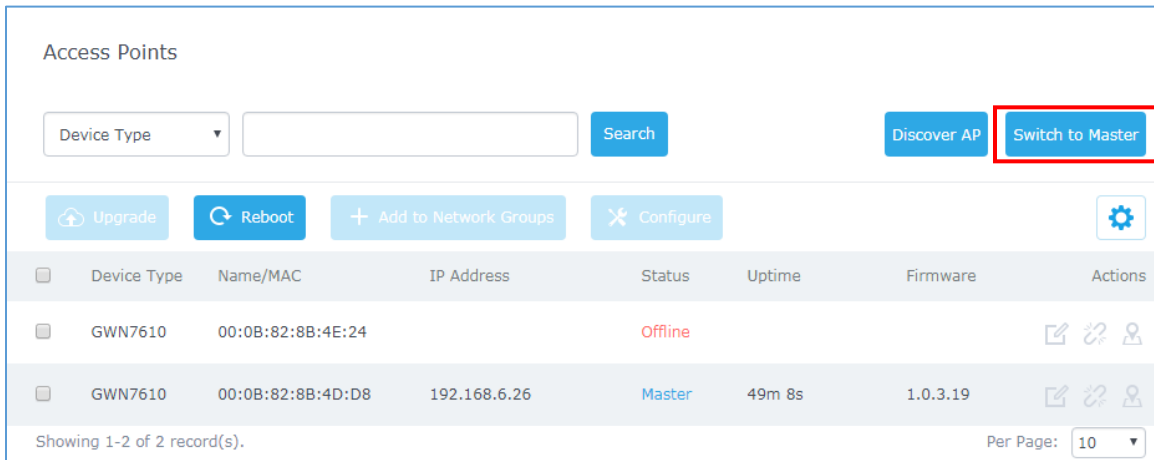
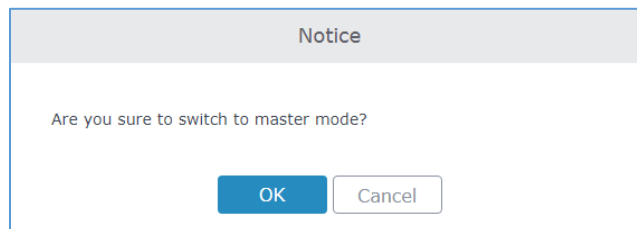


Figure 13 : Switch to Master

The new added button “**Switch to master**” allows users to set the failover slave as the new primary master of the wireless network, once this is done they have full write permission control over the web GUI option as usual.

Note: When the user presses the “**Switch to master**” button, the AP will be set as Master, and will not be able to return to the slave mode automatically, users can set this option when the primary Master is no longer responding. A confirmation message will pop up when the user presses this button:



Once the user confirms and presses OK, the AP will be a Master access point, and users can configure then any option including a new Failover Master:

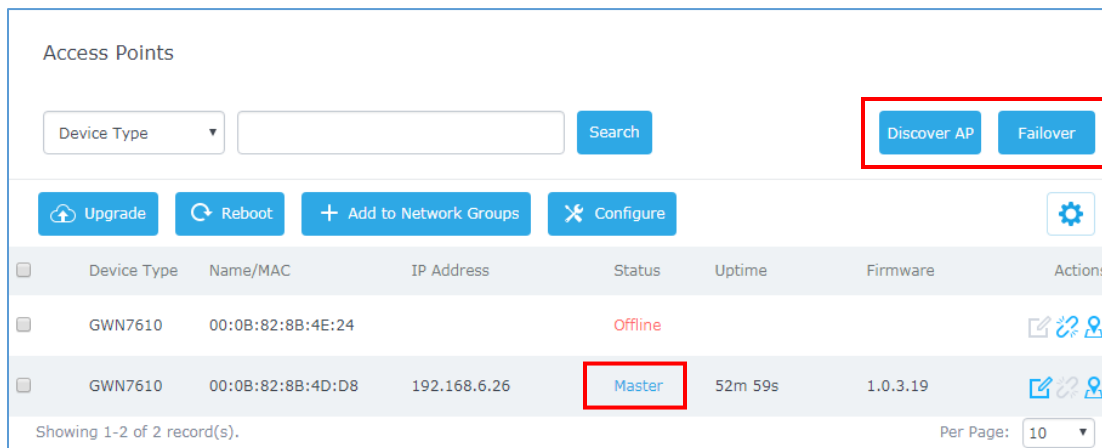


Figure 14 : AP Switched to Master



CREATE AND MANAGE NETWORK GROUPS

After creating Master/Slave architecture using deployed GWN76xx access points, It is possible to create different Network Groups on the Master GWN76xx and select specific GWN76xx Slave Access Points as members in the Network Group.

i

Information

Network Group:
 Each set of devices communicating directly with each other is called a Basic Service Set (BSS). Several BSSs can be joined together to form one logical WLAN segment, referred to as an Extended Service Set (ESS). A GWN76xx network group is an Extended Service Set. A Group also can contain different SSIDs.

SSID:
 A Service Set Identifier (SSID) is the name given to each ESS. It is also the primary name associated with an 802.11 wireless local area network (WLAN) including home networks and public hotspots. Client devices use this name to identify and join wireless networks. SSIDs are case-sensitive text strings. The SSID is a sequence of alphanumeric characters (letters or numbers) with a maximum length of 32 characters.

The following steps show how to create and manage network groups:

1. Login to the Master GWN76xx AP web GUI and navigate to **Network Group**→**Network Group**.

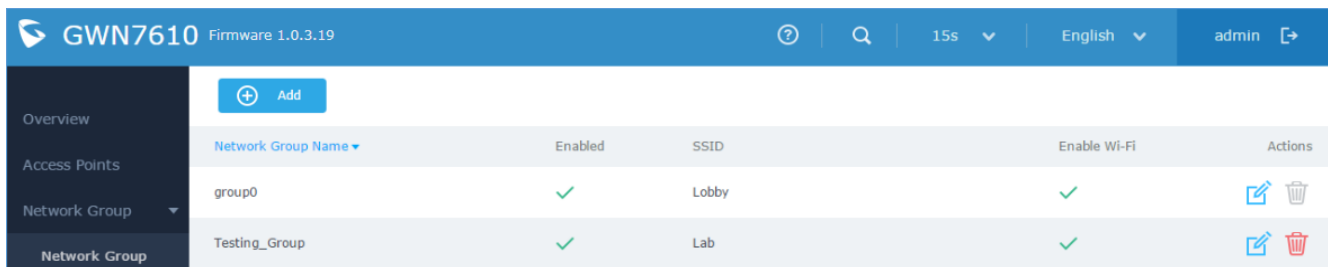


Figure 15: Network Group

2. The GWN76xx has a default network group named **group0** (enabled by default). Click on [Edit](#) to edit it, or click on [Add](#) to add a new network group if needed.

Add
✕

Basic
Wi-Fi
Device Membership

Network Group Name ?

Enabled

VLAN

VLAN ID

Figure 16: Add a New Network Group



Notes:



- A network group can be formed by one or multiple GWN76xx access points (including Master GWN76xx). Each network group can have a unique or different SSIDs (up to 16). A slave access point can be member of different network groups.
- GWN76xx does not support DHCP server and cannot assign IP addresses to devices. GWN76xx acts only as a relay of the router connected to it.

Network Group & SSID Configuration

Network group configuration is available when editing or adding a new network group. The configuration is arranged in 3 tabs including Basic, Wi-Fi and Device Membership.

- **Basic:** This tab allows to define a name to identify the network group, enable or disable VLAN, and specify VLAN ID for the group.

Table 2: Network Group Settings – Basic

Network Group Name	Defines a name for the network group.
Enabled	Enables/disables a network group. group0 is by default enabled.
VLAN	Enables/disables VLAN setting.
VLAN ID	Set VLAN ID when VLAN option is enabled.
Enable IPv4	Check to enable IPv4 addressing for this network group
IPv4 Static Address	Set a static IPv4 address for the network group when enabling IPv4.
Additional IPv4 Static Address	Set an additional static IPv4 address for the network group when enabling IPv4.
IPv4 Subnet Mask	Set the Subnet Mask.
DHCP Enabled for IPv4	Check to enable DHCP using IPv4. This will allow clients connected to this network group to get IPv4 addresses automatically from GWN7000 acting as DHCP server.
DHCP Start Address	Set the starting IPv4 address for this network group's clients.
DHCP End Address	Set the ending IPv4 address for this network group's clients
DHCP Lease Time	Set the lease time for DHCP clients, the value can be defined in hours, minutes, or as "infinite". Default lease time is "12h".
DHCP Options	Set the DHCP options. Click on  to add another option, and  to delete an option. Example: 44,192.168.2.50 for DHCP option 44 and 192.168.2.50 is the WINS server's address. Please refer to the following link for DHCP options syntax: https://wiki.openwrt.org/doc/howto/dhcp.dnsmasq
DHCP Gateway	Defines the IP address of the DHCP gateway.
DHCP Preferred DNS	Set the <u>preferred DNS Servers via DHCP</u> .
DHCP Alternate DNS	Set the <u>alternate DNS Servers via DHCP</u> .

Note: "Enabled", "VLAN" and "VLAN ID" options are available for created network groups only.



- **Wi-Fi:** This tab contains all Wi-Fi settings to be used by the group, including definition of SSID, security mode, MAC filtering...

Table 3: Network Group Settings – Wi-Fi

Enable Wi-Fi	Check to enable Wi-Fi for the network group.
SSID	Set or modify the SSID name.
SSID Band	Select the Wi-Fi band the GWN will use, three options are available: <ul style="list-style-type: none"> • Dual-Band • 2.4GHz • 5Ghz
SSID Hidden	Select to hide SSID. SSID will not be visible when scanning for Wi-Fi, to connect a device to hidden SSID, users need to specify SSID name and authentication password manually.
Wireless Client Limit	Configure the limit for wireless client. If there's an SSID per-radio on a network group, each SSID will have the same limit. So, setting a limit of 50 will limit each SSID to 50 users independently. If set to 0 the limit is disabled.
Enable Captive Portal	Click on the checkbox to enable the captive portal feature.
Captive Portal Policy	Select the captive portal policy already created on the " <i>Error! Reference source not found.</i> " web page to be used in the created SSID.
Security Mode	Set the security mode for encryption, 5 options are available: <ul style="list-style-type: none"> • WEP 64-bit: Using a static WEP key. The characters can only be 0-9 or A-F with a length of 10, or printable ASCII characters with a length of 5. • WEP 128-bit: Using a static WEP key. The characters can only be 0-9 or A-F with a length of 26, or printable ASCII characters with a length of 13. • WPA/WPA2: Using "PSK" or "802.1x" as WPA Key Mode, with "AES" or "AES/TKIP" Encryption Type. • WPA2: Using "PSK" or "802.1x" as WPA Key Mode, with "AES" or "AES/TKIP" Encryption Type. Recommended configuration for authentication. • Open: No password is required. Users will be connected without authentication. Not recommended for security reasons.
WEP Key	Enter the password key for WEP protection mode.
WPA Key Mode	Select key mode (Pre-Shared Key or 802.1X Authentication).
WPA Encryption Type	Select Encryption type (AES or AES/TKIP).
Radius Sever Address	Configures Radius authentication server address.
Radius Server Port	Configures Radius Server Listening port (default is: 1812).
Radius Server Secret	Enter the secret password for client authentication with radius server.



Radius Accounting Server	Configures the address for the radius accounting server.
Radius Accounting Server Port	Configures Radius accounting server listening port (defaults to 1813).
Radius Accounting Server Secret	Enter the secret password for client authentication with radius accounting server.
Use MAC Filtering	Choose Blacklist/Whitelist to specify MAC addresses to be excluded/included from connecting to the zone's Wi-Fi. Default is Disabled.
Enable Dynamic VLAN	When enabled, clients will be assigned IP address form corresponding VLAN configured on the Radius user profile.
Client Isolation	<p>Client isolation feature blocks any TCP/IP connection between connected clients to GWN7600's Wi-Fi access point. Client isolation can be helpful to increase security for Guest networks/Public Wi-Fi.</p> <p>Three modes are available:</p> <ul style="list-style-type: none"> • Internet Mode: Wireless clients will be allowed to access only the internet services and they cannot access any of the management services, either on the router nor the access points GWN7600. • Gateway MAC Mode: Wireless clients can only communicate with the gateway, the communication between clients is blocked and they cannot access any of the management services on the GWN7600 access points. • Radio Mode: <i>Wireless clients can access to the internet services, GWN7xxx router and the access points GWN7600 but they cannot communicate with each other.</i>
Gateway MAC Address	<p>This field is required when using Client Isolation, so users will not lose access to the Network (usually Internet).</p> <p>Type in the default LAN Gateway's MAC address (router's MAC address for instance) in hexadecimal separated by ":".</p> <p>Example: 00:0B:82:8B:4D:D8</p>
RSSI Enabled	Check to enable RSSI function, this will lead the AP to disconnect users below the configured threshold in Minimum RSSI (dBm) .
Minimum RSSI (dBm)	Enter the minimum RSSI value in dBm. If the signal value is lower than the configured minimum value, the client will be disconnected. The input range is from "-94" or "-1".
Enable Voice Enterprise	<p>Check to enable/disable Voice Enterprise. The roaming time will be reduced once enable voice enterprise.</p> <ul style="list-style-type: none"> • The 802.11k standard helps clients to speed up the search for nearby APs that are available as roaming targets by creating an optimized list of channels. When the signal strength of the current AP weakens, your device will scan for target APs from this list. • When your client device roams from one AP to another on the same network, 802.11r uses a feature called Fast Basic Service Set Transition (FT) to authenticate more quickly. FT works with both pre-shared key (PSK) and 802.1X authentication methods.



	<ul style="list-style-type: none"> 802.11v allows client devices to exchange information about the network topology, including information about the RF environment, making each client network aware, facilitating overall improvement of the wireless network. <p>Note: 11R is required for enterprise audio feature, 11V and 11K are optional.</p>
Enable 11R	Check to enable 802.11r
Enable 11K	Check to enable 802.11k
Enable 11V	Check to enable 802.11v
Upstream Rate	Set the maximum upstream rate
Downstream Rate	Set the maximum downstream rate

Edit

Basic
Wi-Fi
Device Membership
Schedule

Enable Wi-Fi

SSID

SSID Band Dual-Band ▼

SSID Hidden

Wireless Client Limit

Enable Captive Portal

Security Mode WPA2 ▼

WPA Key Mode PSK ▼

WPA Encryption Type AES ▼

WPA Pre-Shared Key

Use MAC Filtering Disabled ▼

Client Isolation

Enable Minimum RSSI

Minimum RSSI (dBm)

Save
Cancel

Figure 17: Wi-Fi Settings



- **Device Membership:** This tab lists available devices previously paired and allows to define slave GWN76xx access points as members of the network group.

Click on → to add a paired GWN76xx to the network group, or click on ← to remove it.

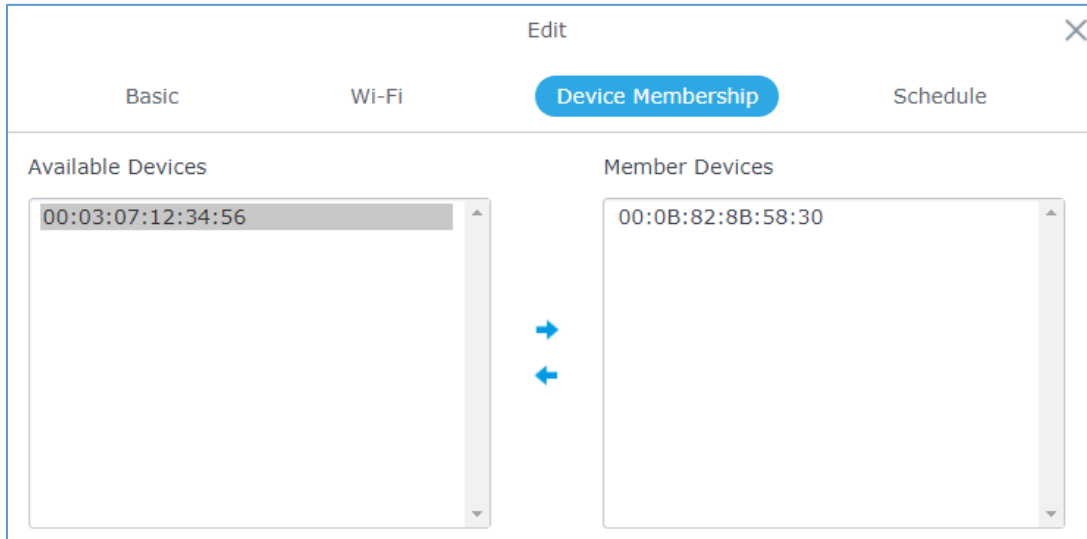


Figure 18: Device Membership

It is also possible to add a device to a Network Group from Access Points Page:

- Select the desired AP to add to a Network Group and click on 

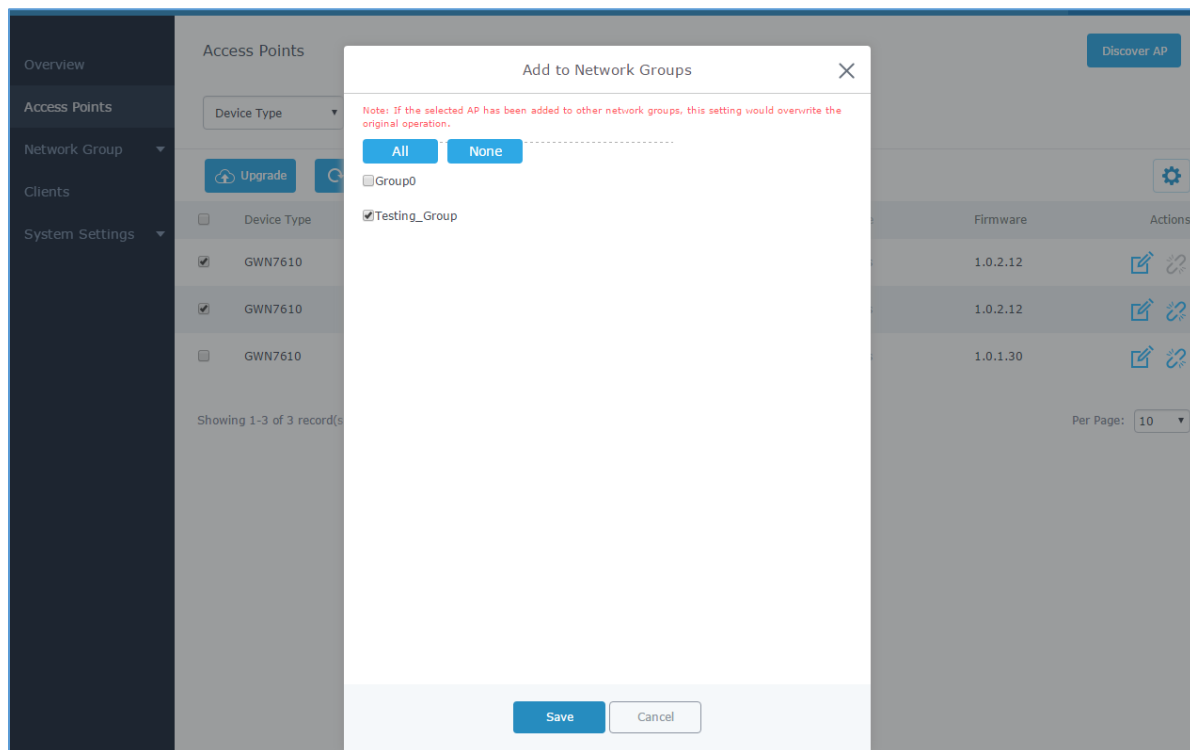


Figure 19: Add AP to Network Group from Access Points Page

- Check to select the desired Network, on which the selected APs will be added, as shown in the above figure.
- **WiFi schedule:** If users want to schedule the AP operation time, “Enable Wireless Schedule” should be selected first, and then, choose the days the AP needs to work, at last, click on “Save” to save configuration.

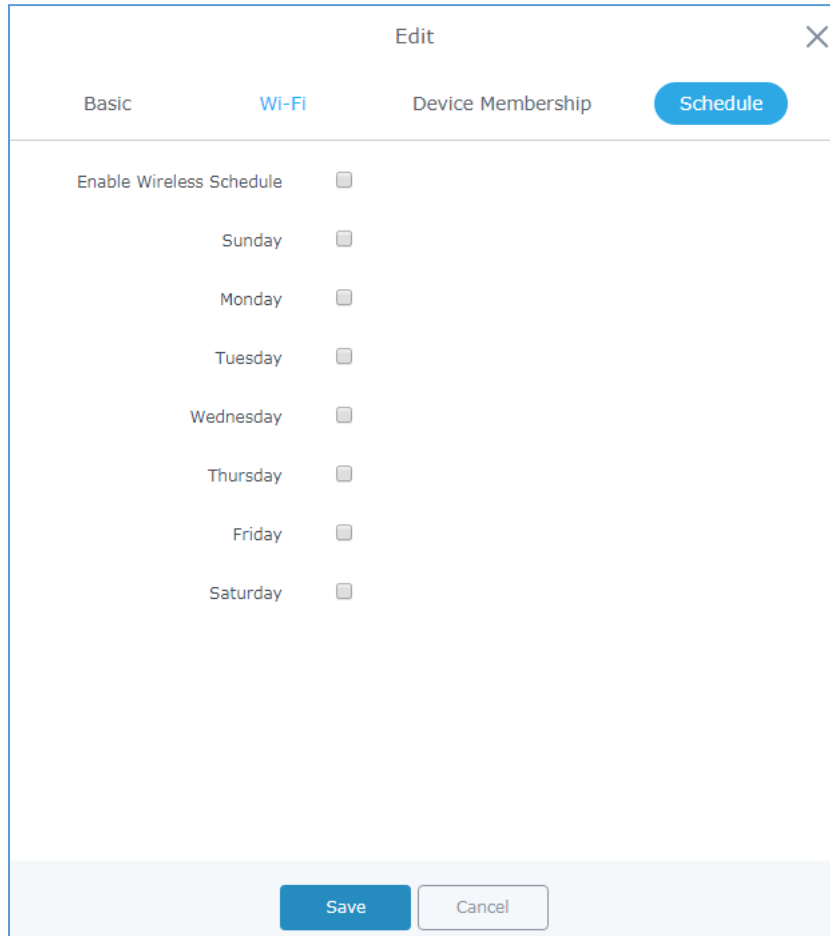


Figure 20: WiFi Schedule Feature

Additional SSID

Additional SSID allows creating multiple SSIDs under the same group including one or multiple GWN76xx access points.

If configured, different SSID will be available for devices within nearest GWN76xx access points range under the same network group.

1. To create an additional SSID go to **Network Group**→**Additional SSID**



Add

Wi-Fi
Schedule

Enable Additional SSID

SSID

SSID Band

Network Group Membership

SSID Hidden

Wireless Client Limit

Enable Captive Portal

Security Mode

WPA Key Mode

WPA Encryption Type

WPA Pre-Shared Key

Use MAC Filtering

Client Isolation

Enable Minimum RSSI

Save
Cancel

Figure 21: Additional SSID

2. Select one of the available network groups from **Network Group Membership** dropdown menu. This will create an additional SSID with the same Device Membership configured when creating the main network group.





SSID	Enabled	Network Group	Hidden	Security Mode	MAC Filtering	Client Isolati...	RSSI	Actions
Additional_SSID	✓	group0	✗	WPA2	Disabled	✗	✗	 

Figure 22: Additional SSID Created

3. Click on  to delete the additional SSID, or  to edit it.

Note: The GWN76xx Series support up to 16 SSID per radio band (2.4G, 5G). This allows creating SSIDs under different groups or on the same group within this limit.

